(ISC)2 Survey Finds Cybersecurity Professionals Being Repurposed During COVID-19 Pandemic

Submitted by: (ISC)² Ltd EMEA
Tuesday, 28 April 2020

47% of respondents have been temporarily taken off security duties to assist with IT-related tasks as organisations move to remote work

Clearwater, FL, April 28, 2020 – (ISC)² – the world's largest non-profit association of certified cybersecurity professionals – today released the findings of a survey in which 256 cybersecurity professionals shared insights into their current work situations during the first several weeks of the COVID-19 pandemic. In the (ISC)2 COVID-19 Cybersecurity Pulse Survey, 81% of respondents, all responsible for securing their organisations' digital assets, indicated that their job function has changed during the pandemic. 90% indicated they themselves are now working remotely full-time.

"The goal of the survey was to take the pulse of the cybersecurity community as many of their organisations began to shift their employee bases and operations to remote work setups in March and April," said Wesley Simpson, COO of (ISC)². "While this was certainly not an in-depth study of the situation, it does provide a current snapshot of the issues and challenges our members may be facing during this unprecedented time. Sharing this information helps our members and other professionals in the field understand the challenges their peers are facing, and hopefully realise they are not alone, even if many of them are feeling isolated as they adjust to working from home."

The (ISC)2 COVID-19 Cybersecurity Pulse Survey's findings shed light on the recent adjustments that organisations have made to maintain their business operations and the impact on cybersecurity professionals. Findings include:

• 96% of respondents' organisations have closed their physical work environments and moved to remote work-from-home policies for employees; nearly half (47%) said this was the case for all employees, while 49% indicated that at least some employees are working remotely
• 23% said cybersecurity incidents experienced by their organisation have increased since transitioning to remote work – with some tracking as many as double the number of incidents
• 81% of respondents said their organisations view security as an essential function at this time
• 47% of respondents said they have been taken off some or all of their typical security duties to assist with other IT-related tasks, such as equipping a mobile workforce
• 15% of respondents indicated their information security teams do not have the resources they need to support a remote workforce, while another 34% said they do, but only for the time being
• 41% said their organisations are utilising best practices to secure their remote workforce, while another 50% agreed, but admitted they could be doing more
• Almost one-third (32%) of respondents were aware of someone in their organisation who has contracted COVID-19

Challenges Facing Cybersecurity Professionals
The survey also asked respondents to share comments about the challenges they face during COVID-19. Some of the themes that came to light included a lack of hardware to support a larger number of remote workers, the struggle between organisational priorities for quick deployment of remote technology and the

commensurate level of security to protect systems, and helping end users understand and abide by security policies outside the office.

One respondent commented, “Security at this point is a best effort scenario. Speed has become the primary decision-making factor. This has led to more than a few conversations about how doing it insecurely will result in a worse situation than not doing it at all.”

A Perfect Recipe for Cybercrime

One respondent summed up the factors that have contributed to an opportune situation for cybercriminals:

“COVID-19 hit us with all the necessary ingredients to fuel cybercrime: 100% work from home [WFH] before most organisations were really ready, chaos caused by technical issues plaguing workers not used to WFH, panic and desire to ‘know more’ and temptation to visit unverified websites in search of up-to-the-minute information, remote workforce technology supported by vendors driven by ‘new feature time to market’ and NOT security, employees taking over responsibilities for COVID-19 affected co-workers (unfamiliarity with process), and uncertainty regarding unexpected communication supposedly coming from their employers.”

Lessons Learned

Several respondents also viewed the pandemic as an opportunity for future process improvement, however, as the following comments illustrate:

“With a majority of the workforce staying home we will all need to rethink our policies and the compromises we are willing to make.”

“People seem to be thinking more about security when they are working remotely, which is a good thing.”

“Employers now face the prospect of doing what they should have done long before: enact contingency plans for large-scale remote work due to natural or man-made disasters. Enabling remote work also has the benefit of appealing to potential employees when recruitment is a concern.”

Looking Forward

The results of the survey will be discussed at 6pm BST (7pm CEST / 1pm EDT) today on an (ISC)2 webinar (https://www.isc2.org/News-and-Events/Press-Room/Posts/ISC2-Webinar-Will-Explore-Cybersecurity-Lessons-Learned-Durin with cybersecurity experts offering their own insights on how the situation has affected their teams.

About the Survey Methodology

Results presented are from an online survey conducted by (ISC)2 in April 2020. The total respondent base of 256 global cybersecurity professionals are responsible for securing their organisations’ digital assets. This survey response sample should not be viewed as statistically representative of the entire cybersecurity workforce. It is intended to share insight with the profession and facilitate sharing best practice and lessons learned during these unprecedented times.

About (ISC)²

(ISC)² is an international non-profit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)² offers a portfolio of credentials that are part of a holistic, pragmatic approach to security. Our membership, more than 150,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry. Our vision is supported by our commitment to educate and reach the general public through our charitable foundation – The Center for Cyber Safety and Education (https://www.iamcybersafe.org/)™. For more information on (ISC)², visit www.isc2.org, follow us on Twitter (https://twitter.com/isc2) or connect with us on Facebook (https://www.facebook.com/isc2fb) and LinkedIn (https://www.linkedin.com/company/isc2).

###

--

Chris Green
Head of PR and Communications – EMEA
(ISC)²
Tel: +44 203 960 7812
Email: cgreen@isc2.org